Chair for Security in Information Technology
Department of Electrical and Computer Engineering
Technical University of Munich

PUF Key Storage Based on $BiFeO_3$ Memristors

Jonas Ruchti[1], Danilo Bürger[2], Nan Du[2,3,4], Michael Pehl[1], Heidemarie Schmidt[3,4]

[1] Technische Universität München, Arcisstr. 21, 80333 München; [2] Fraunhofer ENAS, Technologie-Campus 3, 09126 Chemnitz; [3] FSU Jena, IFK, Helmholtz-Weg 5, 07743 Jena; [4] Leibniz-IPHT, Albert-Einstein-Str. 9, 07745 Jena

MOTIVATION

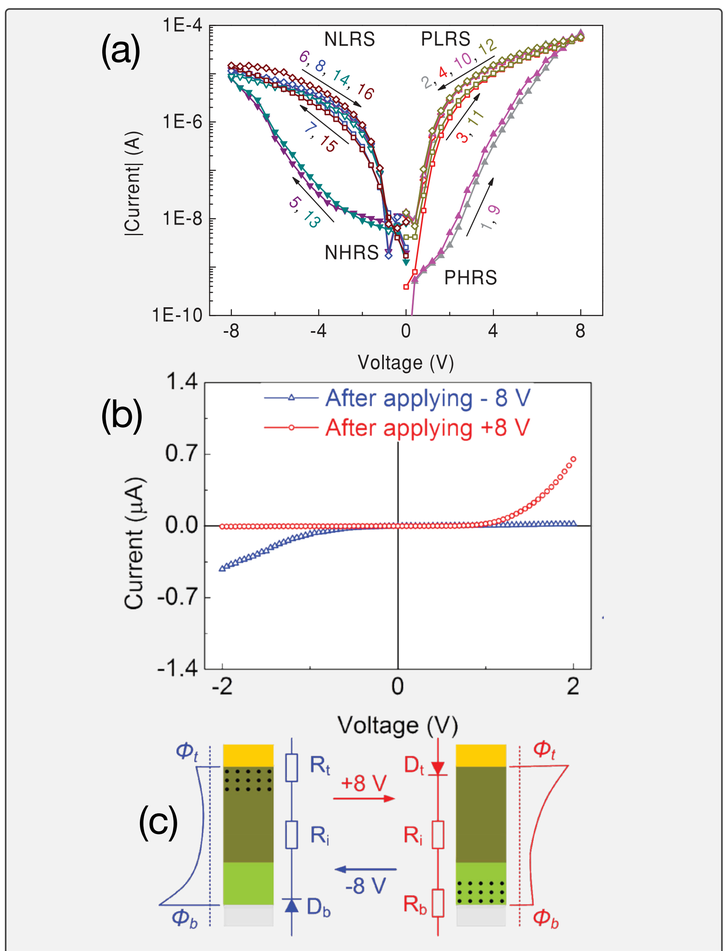
- Moore's law is slowing down for CMOS fabrication and new technologies need to be investigated.
- Memristors promise very high integration densities and good power efficiency.
- Physical Unclonable Functions (PUFs) are of rising importance, especially in the Internet-of-Things (IoT) domain.

Different memristor-based PUFs have been proposed. Apart from hybrid CMOS-memristor PUF designs, measurements of manufacturing differences in the

- resistance for a known memristor state [1] (W/SiGe),
- write pulse response [3] (TiO_x), and
- dynamic write current [2] (TiO_x/Al_2O_3)

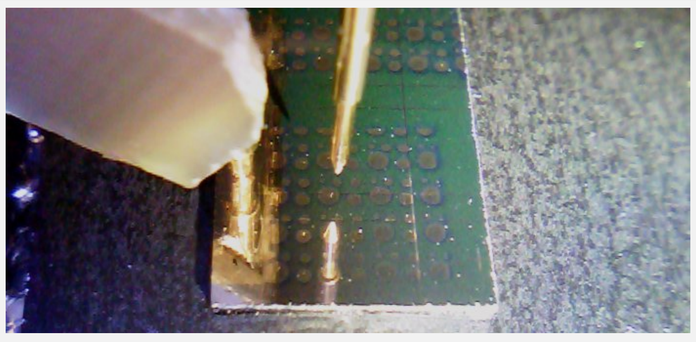
have been used as entropy sources.

Among the known memristors, the electroforming-free $BiFeO_3$ (BFO) memristors offer simplified crossbar construction because of their inherent self-rectifying behaviour. However, it remains to be shown which PUF construction is optimal for BFO memristors.



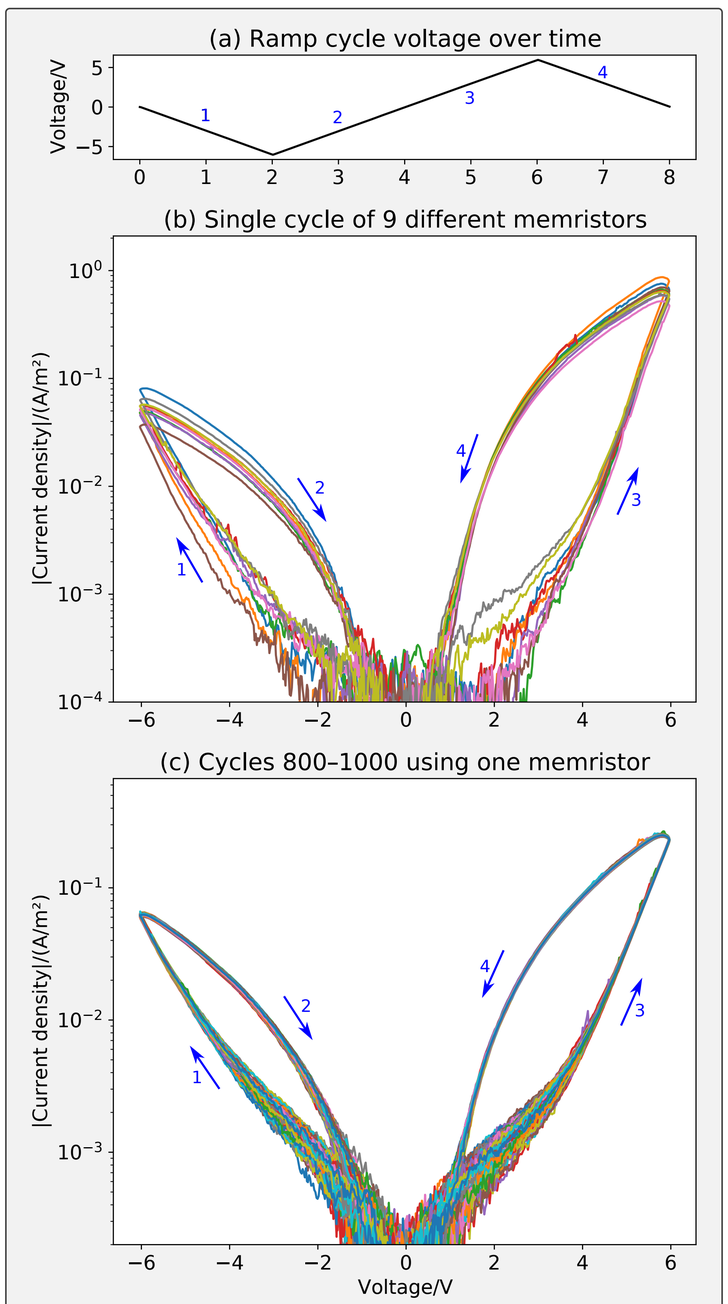
(a) Double hysteresis in the current-voltage characteristic curves of a BFO memristor. (b) Diode-like behaviour in the reading bias range from -2 V to +2 V and equivalent circuit model (c) for two states of the reconfigurable top and bottom electrodes. Figure adapted from [4].

PRELIMINARY WORK ON BFO MEMRISTORS



Photograph of a BFO memristor die with unstructured bottom electrode and circular top electrodes with different diameters within the measurement set-up.

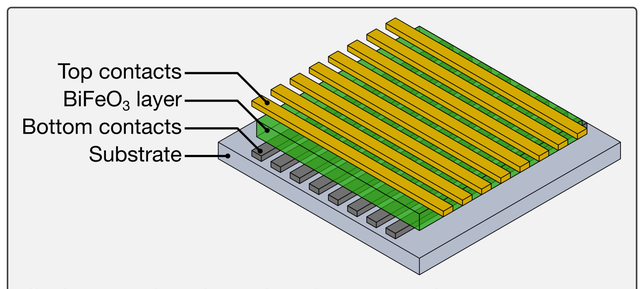
- Variability in the dynamic write current has been investigated.
- Diode behavior with two reconfigurable barriers (top and bottom electrodes) has been confirmed.
- Inter-device variability and cycle-to-cycle reproducibility has been shown for a small number of devices and for more than 500 cycles.



Measurement results using a voltage profile over an 8 s period (a). (b), using 9 memristors, highlights the sample variability, corresponding to high PUF entropy. 200 cycles using the same memristor (c) demonstrate the high reliability and thus promise a small bit error rate.

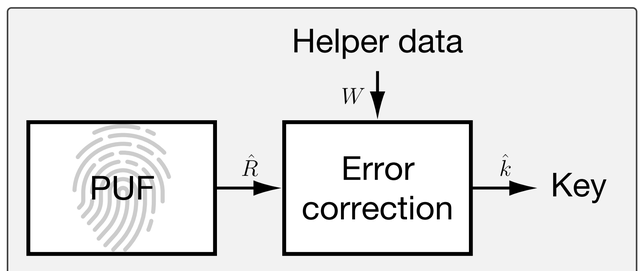
OUTLOOK

- Design of suitable quantisation methods to best reveal the BFO memristors' manufacturing variability, ensuring high reliability.
- Realisation of BFO memristor PUFs on crossbar arrays.



Schematic sketch of a crossbar structure with BFO memristors at the crosspoints.

- Development of a BFO PUF key storage module optimised for low bit error rate and energy consumption, and high available key entropy.
- Design of novel key derivation algorithms exploiting the specific properties of BFO memristor PUFs to minimise the need for helper data.



Simplified conventional PUF key storage scheme.

- Assessment of physical (fault, side-channel) attacks on a constructed BFO PUF key storage module.

REFERENCES

[1] Wenjie Che, Jim Plusquellic and Swarup Bhunia. 'A non-volatile memory based physically unclonable function without helper data'. In: *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, Nov. 2014.

[2] Dayoung Kim et al. 'Selected Bit-Line Current PUF: A Non-Invasive Hardware Security Primitive Based on a Memristor Crossbar Array'. In: *IEEE Access* (2021), pp. 1–1.

[3] Garrett S. Rose et al. 'A write-time based memristive PUF for hardware security applications'. In: *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, Nov. 2013.

[4] Tiangui You et al. 'Exploiting Memristive BiFeO3 Bilayer Structures for Compact Sequential Logics'. In: *Adv. Funct. Mater.* 24.22 (June 2014), pp. 3357–3365. ISSN: 1616-301X.